LAWYERS

Davis Wright Tremaine LLP

ANCHORAGE BELLEVUE LOS ANGELES NEW YORK PORTLAND SAN FRANCISCO SEATTLE SHANGHAI WASHINGTON, D.C.

PAUL HUDSON
DIRECT (202) 973-4275
paulhudson@dwt.com

SUITE 200
1919 PENNSYLVANIA AVE NW
WASHINGTON, DC 20006

TEL (202) 973-4200
FAX (202) 973-4499
www.dwt.com

February 27, 2009

VIA ELECTRONIC FILING

Marlene H. Dortch
Office of the Secretary
Federal Communications Commission
445 12th Street, S.W.
Washington, D. C. 20554

Re: EB Docket 06-36, Annual 47 C.F.R. § 64.2009(e) CPNI Certification

Annual § 64.2009(e) CPNI Certification for 2008
Date filed: February 27, 2009
Name of companies covered by this certification and Form 499 Filer IDs:

Northland Communications Corporation.	
Northland Cable Properties, Inc.	**826515**
Northland Cable Television, Inc.	**826497**
Northland Cable Ventures LLC	**826517**
Northland Cable Properties Eight L.P.	**826519**
Northland Cable Properties Seven L.P.	**826518**

Name of signatory: **Paul Milan**
Title of signatory: **Vice President and General Counsel**

Dear Ms. Dortch:

Pursuant to Section 64.2009(e) of the Commission's Rules, 47 C.F.R. § 64.2009(e), enclosed for filing in the above-referenced docket is the executed annual CPNI Compliance Certificate of Northland Communications Corporation and its affiliates listed above (together, "Company").

Attached to the certificate is a summary of Company's CPNI policies and procedures. Because some of the details included in that document could provide a roadmap for unauthorized persons to attempt to obtain CPNI, Company is filing only a redacted version with the

Commission's electronic filing system and has provided the non-redacted version of this filing directly to the Enforcement Bureau. *See Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, Report and Order and Further Notice of Proposed Rulemaking, FCC 07-22, n. 167 (rel. April 2, 2007) ("We recognize carrier concerns about providing a roadmap for pretexters with this annual filing, and thus we will allow carriers to submit their certifications confidentially with the Commission."). Accordingly, pursuant to Section 0.459 of the Commission's Rules, 47 C.F.R. § 0.459, Company is concurrently submitting a request that the non-redacted version be designated by the Commission as confidential and not be made routinely available for public inspection.

Please note that Company's prior year certificate was also submitted on behalf of Northland Cable Networks LLC, 499 Filer ID # 826516. Company no longer provides interconnected VoIP services through that entity.

Respectfully submitted,

Paul B. Hudson
Counsel for Northland Communications Corp.

Enclosures

Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2008
Date filed: February 27, 2009
Name of companies covered by this certification and Form 499 Filer IDs:

Northland Communications Corporation	
Northland Cable Properties, Inc.	**826515**
Northland Cable Television, Inc.	**826497**
Northland Cable Ventures LLC	**826517**
Northland Cable Properties Eight Limited Partnership	**826519**
Northland Cable Properties Seven Limited Partnership	**826518**

Name of signatory: **Paul Milan**
Title of signatory: **Vice President and General Counsel**

I, Paul Milan, certify that I am an officer of Northland Communications Corp., the manager of Northland Cable Properties, Inc.; Northland Cable Television, Inc.; Northland Cable Ventures, LLC; Northland Cable Properties Eight Limited Partnership; and Northland Cable Properties Seven Limited Partnership (together, the "Company"), and, acting as an agent of each of these companies, that I have personal knowledge that the Company has established operating procedures, summarized in the attached statement, that are adequate to ensure compliance with the Commission's rules governing use and disclosure of confidential proprietary network information ("CPNI"), as governed by Section 222 of the Communications Act of 1934, as amended by the Telecommunications Act of 1996, and as set forth in Part 64, Subpart U of the of the Commission's rules, 47 C.F.R. §§ 64.2001 *et seq.*

The Company has not received any customer complaints in the past calendar year concerning unauthorized access to or release of CPNI. The Company does not have any material information with respect to the processes pretexters are using to attempt to access CPNI that is not already a part of the record in the Commission's CC Docket No. 96-115. Company has therefore not taken any actions in the past year against data brokers, including proceedings instituted or petitions filed by the company at either state commissions, the court system or at the Commission. The Company has established procedures to report any breaches to the FBI and United States Secret Service, and it has emphasized in its employee training of the need for vigilance in identifying and reporting unusual activity in order to enable the Company to continue to take reasonable measures to discover and protect against pretexting and other unauthorized access to CPNI.

Paul Milan
Vice President and General Counsel
Northland Communications Corp.
Executed February 27, 2009

Gr07a

PUBLIC VERSION

Northland Communications Corporation dba Northland Cable Television – Consumer Proprietary Network Information Policy

Revised Effective June 8, 2008

This document, the Northland Communications Corporation dba Northland Cable Television Consumer Proprietary Network Information Policy (the "Policy"), sets forth Northland Communications Corporation dba Northland Cable Television and its affiliates' (collectively, "Northland" or the "Company") policies and procedures regarding the protection and use of Consumer Proprietary Network Information ("CPNI"). CPNI is defined as follows:

> (A) information that relates to the quantity, technical configuration, type, destination, location and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and
> (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier.

The following Policy is designed to protect the confidentiality of CPNI and assure compliance with the Federal Communications Commission's ("FCC") rules set forth in 47 C.F.R. Part 64, Subpart U, Section 2001 *et seq*., including, but not limited to, the new rules adopted in *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, Report and Order and Further Notice of Proposed Rulemaking, FCC 07-22 (rel. April 2, 2007). To ensure compliance, the Company trains employees on the limitations of use or disclosure of CPNI as governed by Federal law and the Policy. The Policy is administered by its CPNI Compliance Officer, Paul Milan, General Counsel, located at 101 Stewart Street, Suite 700, Seattle, Washington 98101; Phone: (206) 621-1351; Fax: (206) 748-5061; email: paul@northlandco.com.

Because the details of this policy could provide a roadmap for unauthorized persons to attempt to subvert these policies and attempt to obtain CPNI, copies of this policy and related training materials are classified as confidential and may be provided only to Company employees or to parties approved by the CPNI Compliance Officer. [REDACTED]

I. USE, DISCLOSURE OF, AND ACCESS TO CPNI

Company will use, disclose or permit access to individually identifiable CPNI only as follows:

- in its provision of the communications service from which such information is derived;
- for services necessary to, or used in, the provision of such communications service, including the publishing of directories;
- to initiate, render, bill and collect for communications services; to protect the rights or property of the Company, or to protect users or other carriers or service providers from fraudulent or illegal use of, or subscription to, such services;

- to provide inbound marketing, referral or administrative services to the customer for the duration of the call, if the call was initiated by the customer and the customer approves of the carrier's use to provide such service;
- to provide inside wiring installation, maintenance or repair services;
- as required by law; or
- as expressly authorized by the customer.

Company does not use CPNI for outbound marketing of service offerings among the different categories of service or within the same category of service that it provides to subscribers. If the Company changes the Policy, Company shall conduct additional training as needed to assure compliance with the FCC's rules. Company does not use, disclose or permit access to CPNI to identify or track customers that call competing service providers.

II. SAFEGUARDS AGAINST DISCLOSURE OF CPNI TO UNAUTHORIZED PARTIES

Company takes reasonable measures to protect against attempts to gain unauthorized access to CPNI. Company Customer Service Representatives ("CSRs") are trained in procedures emphasizing, among other points, [REDACTED]. If any CSR becomes aware of new methods that are being used or could be used by third parties to attempt to obtain unauthorized access to CPNI, or of possible changes to Company's existing policies that would strengthen protection of CPNI, the CSR is instructed to report such information immediately to Company's CPNI Compliance Officer.

A. Online Accounts

Company makes CPNI available to customers through Company's online service location. The website contains billing information, including phone, Internet, video and ancillary services billing information, and has tools that allows the customer to customize their calling features.

Company has implemented the following procedures to safeguard online access to CPNI: [REDACTED].

B. Inbound Calls to Company Requesting CPNI

CSRs may not disclose any CPNI to an inbound caller until the caller's identity has been authenticated. The customer's identity is authenticated by obtaining account number and/or service location information. All callers requesting Call Detail Information ("CDI") CPNI are first directed to their online account. Company does not provide CDI-CPNI over the phone on an inbound call. If a customer is able to provide to the CSR the telephone number called, when it was called, and, if applicable, the amount charged for the call, exactly as that information appears on the bill, then the CSR is permitted to discuss customer service pertaining to that call and that call only. [REDACTED].

The CSR may offer to call the caller back at the customer's telephone number of record. The CSR may not rely on Caller ID information to assume that the caller is calling from such

number; they must disconnect the inbound call and make a new outbound call to the number of record. The CSR may offer to send a copy of a bill or requested CDI to a mailing address of record for the account, but only if such address has been on file with Company for at least thirty (30) days.

[REDACTED]

C. In-Person Disclosure of CPNI at Company Offices

Company may disclose a customer's CPNI to an authorized person visiting a local Company office upon verifying that person's identity through a valid, non-expired, government-issued photo ID (such as a driver's license, passport or comparable ID) matching the customer's account information.

D. Notice of Account Changes

When an online account is created or when a Password is changed, Company will send a notice to customer's address of record notifying them of the change. When an address of record is created or changed Company will mail letters to customer's former address of record notifying them of the change. This notification is not required when the customer initiates service. Each of the notices provided under this paragraph will direct the customer to notify Company immediately if they did not authorize the change.

E. Company Access to CPNI and Audit Trail

[REDACTED]

III. REPORTING CPNI BREACHES TO LAW ENFORCEMENT

The Company acknowledges that Federal law imposes specific requirements upon Company in the event that Company becomes aware of any breach of customer CPNI. A breach includes any instance in which any person has intentionally gained access to, used or disclosed a Company customer's CPNI beyond their authorization to do so. Any Company employee that becomes aware of any breaches, suspected breaches or attempted breaches must report such breach, suspected breach or attempted breach immediately to the Company CPNI Compliance Officer, and such breach, suspected breach or attempted breach must not be reported or disclosed by any employee to any non-employee, including the potentially affected customer or any member of the media, except in express conformance with the procedures described below. Any employee that fails to report such information to the Company CPNI Compliance Officer will be subject to disciplinary action that may include termination. It is Company's policy that employees should not be discouraged from reporting information about breaches that may have been caused in part by their own actions or omissions. Once a breach has occurred, Company's most important objective is to attempt to limit the damage to Company's customers, make any adjustments as needed to prevent a recurrence of the breach and to alert law enforcement promptly. Therefore, although employees who violate the Company's CPNI compliance procedures are subject to

discipline, the sanctions may be substantially reduced when employees promptly self-report violations, if appropriate.

Company's CPNI Compliance Officer is currently Paul Milan, General Counsel, who may be contacted at (206) 621-1351.

A. Identifying a "Breach"

A "breach" has occurred when a person, without authorization or exceeding authorization, has intentionally gained access to, used or disclosed CPNI. If an employee has information about an incident and is not certain that the incident would not constitute a breach under this definition, the incident must be reported to the CPNI Compliance Officer.

B. Notification Procedures

As soon as practicable, and in no event later than seven (7) business days upon learning of a breach, the Company CPNI Compliance Officer shall electronically notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) by accessing the following link: http://www.fcc.gov/eb/cpni. If this link is not responsive, the Company will contact the FCC's Enforcement Bureau (202-418-7450) for instructions.

Company will not, under any circumstances except as provided below, notify customers or disclose a breach to the public until seven (7) full business days have passed after notification to the USSS and the FBI. (A full business day does not count the business day on which the notice was provided.) Federal law requires compliance with this requirement even if state law requires disclosure.

If Company receives no response from law enforcement after the 7th full business day, Company shall promptly inform the customers whose CPNI was disclosed as a result of the breach. The Company is not required to inform customers whose CPNI was not actually disclosed.

Company will delay notification to customers or the public upon request of the FBI or USSS. If the Company CPNI Compliance Officer believes there is a need to disclose a breach sooner, he or she should so indicate in the notification to law enforcement. However, such notification does not itself permit notice to customers; Company still may not notify customers sooner unless given clearance to do so from *both* the USSS and the FBI.

IV. RECORD RETENTION

The Company CPNI Compliance Officer is responsible for maintaining a record, electronically or in some other manner, covering any breaches discovered, notifications made to the USSS and the FBI, and notifications of breaches made to customers over the prior two-year period. The record must include, if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach and the circumstances of the breach.

The Company maintains a record, covering the prior year, of (i) circumstances in which CPNI is disclosed or provided to third parties, or where third parties were allowed access to CPNI, and (ii) supervisory review of marketing that proposes to use CPNI or to request customer approval to disclose CPNI.

Company maintains a record of all customer complaints related to Company's handling of CPNI, and records of the Company's handling of such complaints, for at least two years. The CPNI Compliance Officer will assure that all complaints are reviewed and that the Company considers any necessary changes to its policies or practices to address the concerns raised by such complaints.

Company will have an authorized corporate officer, as an agent of the Company, sign a compliance certificate on an annual basis stating that the officer has personal knowledge that the Company has established operating procedures that are adequate to ensure compliance with FCC's CPNI rules. The certificate for each year will be filed with the FCC Enforcement Bureau in EB Docket No. 06-36 by March 1 of the subsequent year, and will be accompanied by a summary or copy of this Policy that explains how the Company's operating procedures ensure that it is or is not in compliance with the FCC's CPNI rules. In addition, the filing will include an explanation of any actions taken against data brokers and a summary of all customer complaints received in the past year concerning the unauthorized release of CPNI.

V. TRAINING

Company employees must use a unique login and password to obtain access to databases that include CPNI. All employees with such access receive a copy of the Company's CPNI policies and are informed that (i) any use or disclosure of CPNI or other act or omission not in compliance with such policies will result in disciplinary action, including the termination of employment where appropriate, and (ii) employees who knowingly facilitate the unauthorized disclosure of a customer's confidential information may be subject to criminal penalties. In addition, Company requires CPNI training for all CSRs and personnel at retail offices that may receive requests for CPNI and marketing personnel. [REDACTED]